# Improved Device Discovery in Bluetooth Networks

**Niti Singhal[1] and Dr. Kausar Ali[2]**

[1]Vivekananda Institute of Technology, Jaipur, India
niti1980singhal@gmail.com

[2]Vivekananda Institute of Technology, Jaipur, India
kausarali@gmail.com

**ABSTRACT:** ***Security has become a critical requirement for IoT deployments. Key challenges in wireless mobile ad hoc networks are computational resource constraints, power limitations, and efficient service discovery techniques. The short-range radio network technology Bluetooth suffers from long service discovery delays and high-power consumption due to necessary connection establishment between discovering and discovered entity. Therefore, in order to enhance the security, as well as improving the discovery process, the best alternative is Frequency Hop Spread Spectrum (FHSS), which is already employed in Bluetooth discovery, but rather required to be improved. Current BLE transmitters are susceptible to selective jamming due to long discovery times for a channel. To mitigate these constraints, we propose physical-layer security through a Bit Level Fast Frequency-Hopping (BLF FHSS) scheme. It can be seen in simulation, that the hopping frequency estimation performance of our proposed method is the best, and its running time is shortest.***

**KEYWORDS:** Service discovery, FHSS, BLF FHSS, SSMA.

*Article Received: 10 August 2020, Revised: 25 October 2020, Accepted: 18 November 2020*

## 1. INTRODUCTION

The Bluetooth is a new conception which is derived from the 10th century Denmark king Harold Bluetooth. As we know that Bluetooth is a distinguished topic for young network researchers who like to implement wireless networking applications. The Bluetooth is a methodology which supports for squat extent wireless data and also real time Bi-directional voice transfer cooperating instruments.

To the best of our knowledge the Bluetooth technology is made up of different protocol spells which ranges from physical radio and baseband to an object swap and service discovery. The BSIG cataloguing also specifies number of profiles which satisfies the criteria of messages, procedures and protocols essential for supporting a specific service. It is clear that the Bluetooth is a de facto standard for local wireless communication network is one which enables the user either by introducing Point-to-Point connection type or Point to Multipoint Communication type.

A Piconet is a kind of network which consists of Bluetooth devices created by two or more Bluetooth units sharing a homogeneous kind of communication route. The Bluetooth cable replacement protocol for wireless connectivity is made up of one master device and active seven slave equipment. The heterogeneous kind of piconets connected in a huge scale network establishes a scatter net.

## 2. MOTIVATION

Wireless communication technology has advanced at a very fast pace during the last years, creating new applications and opportunities. In addition, Bluetooth technology is wireless and automatic and has a number of interesting features that can simplify our daily lives. Service Discovery in the Bluetooth environment, where the set of services that are available changes dynamically based on the RF proximity of devices in motion, is qualitatively different from service discovery in traditional network- based environments. The service discovery protocol is intended to address the unique characteristics of the Bluetooth environment. Xiaopeng Tana et al. [18] has proposed a narrowband interference suppression technology based on spread spectrum communication. The simulation results show that the method has a good

effect on narrowband interference suppression, and provides an effective solution to the problem of narrowband interference suppression in UAV network

### 2.1 Literature

Igor Sedov et al. [3] stated that, the coordinator collects service information from devices within the community. It uses native Bluetooth SDP to discover existing services and registers these in its own database [2]. Thereafter, it provides the complete community service information.

Rozeha A. Rashid et al. [6] measured the data in the form of different sizes of files, types of files and separation distance against the transmission delay. It is also observed that with obstacles, the propagation of signal transmitted will have more delay regardless of the different sizes of file. It is proved that with two walls in between, the delay is higher for all file sizes.

Bin Zeng et al. [14] used the Randomized algorithms. Neighbor discovery and connection establishment in Bluetooth use asymmetric protocols in the sense that two Bluetooth devices must be in complementary states in order to discover each other and establish connection. Since the neighbor discovery and connection establishment is essentially asymmetric, the program executed by each device must allow the devices to choose to enter INQUIRY state, or enter INQUIRY SCAN state. Therefore, this paper proposed a discovery timeout computation algorithm to help to determine the random process.

ZHAO Tonggang et al. [15] has utilized a new frequency hopping algorithm based on the long distance of wireless sensor network. Frequency hopping sequences will be controlled through the self-designed clock synchronization mode.

Yun He et al. [16] proposed the double window spectrogram difference method, which can eliminate the cross-terms of FH signals and greatly improve the resolution of FH signals. Meanwhile, the running time of this method is short with less computational complexity. The main idea is performing double window spectrogram analysis on the FH signals by using two different window lengths to obtain its hopping frequency, and then based on the frequency analysis of FH signals, the first-order differential processing is used to obtain the hopping period.

## 3. PROBLEM STATEMENT

Threats are also called as Risks which are always creating challenges of different categories in wireless technologies. One of the crucial threats in wireless network is when the prime communication medium is open to all an authorized user as well as the intruders.

Gaoyang Shan et al. [17] has proposed an analytical model to evaluate Advance Neighbor Discovery Process (A-NDP) performances such as the signal collision probability, the discovery delay, the energy consumption and so on. With the proposed analysis model, the performances of A-NDP are analyzed from the viewpoint of various operational environments for BLE enabled IoT services, and compared to those of Basic-NDP (B-NDP) with extended features of Bluetooth 5.0. Besides, it showed that A-NDP is not always better than B-NDP.

### 3.1 Device Discovery Inquiry

The authentication in Bluetooth queries is mainly used to confirm the accordance of one piconet device with another instrument. The resultant output of an authentication mechanism is primarily used to determine authorization spell of a client system. The encryption mechanism also takes an opportunity to transform any Plain Text message into its equivalent cipher text message. When a couple of Bluetooth instruments are commenced to form pairing with the homogeneous PIN (Personal Identification Number) code which is used to create different 128-bit keys as shown in figure 1.

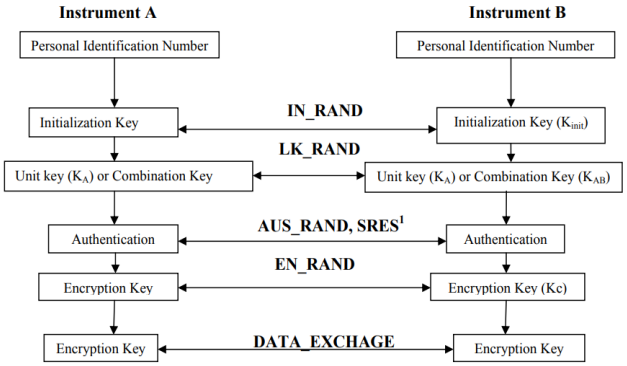


**Figure 1** Gray image and achieved Segments

In Bluetooth security operations the Initialization Key (IK) is mainly availed when Bluetooth apparatus meets first time. It is maneuverer securing the creation of other more secure 128-bit keys which are formed during the next spells of the security chain of the events. As we understood the IK is originated from a 128-bit pseudorandom number IN_RAND and L-byte (1<=L<=16) PIN (Personal Identification Number) and a BD_ADDR. It is confirmed that the IN_RAND is transmitted via air in unencrypted form. The output of certain key creation functions is mainly used in terms of function and its inputs itself.

In both the Bluetooth instruments the IK function is derived by using the general formula:

*IK=E22 (PIN1, L1, IN_RAND)*
*…… (1)*

We have also divided PIN CODE into two different quantities, such as- $PIN_1$ and $L_1$ before forwarding them to the $E_{22}$ function. If suppose the length of PIN is less than 16 bytes, it is elongated by appending bytes from the BD_ADDR instrument until the PIN reaches the total length of 16 bytes or the entire BD_ADDR is pasted, whichever comes first. When one instrument has a fixed PIN code then the Bluetooth address BD_ADDR of the other instrument is used. If both the instruments support a variable PIN code of the BD_ADDR of the instrument which receives an IN_RAND. The IK is used to encrypt a
128-bit Pseudorandom number (RAND or LK_RAND) i.e.,
RAND⊕IK or LK_RAND⊕IK swapped in the next level

sequence of events when a link key is created.

## 4. PROPOSED ALGORITHM

Different kinds of Security measures have been designed and implemented at different protocol phases; but however basic Bluetooth security configuration dependent on the user's Bluetooth Device, who predicts about the discoverability and connection options.

### 4.1 Spread Spectrum Multiple Access

SSMA [10] is one among the Multiple Access techniques in communication systems, that works by expanding the transmitted signal bandwidth to be larger than the bandwidth of the information signal. Spread Spectrum systems [10] are utilized in various fields because of their characteristics which can solve interference problems. Receiver synchronization, is that the foremost complex stage in Spread Spectrum systems, requiring complex circuits and processes [5] [6]. Spread spectrum communication could also be a way of transmitting information [13]. Generally, there are two methods of Spread Spectrum, namely: Direct Sequence Spread Spectrum (DSSS) [9] and Frequency Hopping Spread Spectrum (FHSS).

The utilization of spread spectrum techniques allows multiple simultaneous access and increases the robustness of the system against multipath-induced distortion and narrowband interference [5] DSSS and FHSS. DSSS [9] [11] transmits signals at one frequency but on very wide bands, while FHSS transmits signals with narrow bands, but quickly jumps from one frequency to subsequent [7]. the foremost difference is in how they spread the information into the broader bandwidth [13]. FHSS utilizes frequency hopping while DSSS utilizes pseudo noise to switch the phase of the signal [9] [10].

Frequency Hopping is accomplished by

partitioning the enormous data transmission into more modest channels which can fit the data. It does as such by bringing pseudo- irregular commotion into the sign to shift its stage at some random time. This leads to an output that closely resembles static noise and would seem as just that to others. But with a process called "de-spreading," the first signal is typically extracted from the noise as long because the pseudo- random sequence is understood. DSSS [11] execution better regarding cost and this strategy is perceived most effectively usage, while FHSS prevalent in narrowband obstruction, co-area channel and security [4] [7] [8].

**Table 1:** Mean Delay Spread in different kinds of environments.

| S. | Types of environment | Delay spread (in μ sec) |
|---|---|---|
| 1 | Inside the building | < 0.1 |
| 2 | Open area | < 0.2 |
| 3 | Sub-urban area or city boundary | 0.5 |
| 4 | Urban area or inside the city | 3 |

Fading is produced by interference between two or more versions of the transmitted signal that arrives at receiving device at different times. In wireless radio environment, as a result of multipath reflection phenomenon, the signal transmitted from transmitter and receives at the receiver device will be propagate through different paths. Each of the path has a different length and the time of arrival for each part is different. For example, if an impulse is transmitted from transmitter. At the receiver unit it will be not an impulse but it is a pulse with a spread width and called Delay Spread. The measured data indicates that the mean Delay Spread are different in different kinds of environment. Usually, optimum system performance in noise obtains, when the normalized delay spread is between 0.05 and 0.3 [1].

## 5. RESULTS AND DISCUSSION

A system is taken under consideration to be slow hopping if the hopping rate is smaller than the data-rate. When the hopping rate is quicker than the data rates the system is known as Fast hopping [10]. Simulation study by using MATLAB software as a digital signal processing tool has been exhausted the proposed work. Now, let us see the difference between Frequency Hopping Spread Spectrum and FDM is there with respect to time, how frequency is getting selected that is what we will be explaining. So, in Frequency Division Multiplexing, channel will not change frequency. If there is a channel 1 so channel which will not change frequency with respect to time. The same steps may be applied for all the channels in frequency division multiplexing technique. No any channel will change the frequency over the complete communication.

### 5.1 Modulation Techniques in FHSS

There are some very effective digital modulation methods like FSK, QAM and PAM. The sub-carriers may be modulated with BPSK, QPSK, 16QAM or 64QAM, depending on the data rate requested [19]. But why we do select PSK instead of these effective methods? The reason is that, these methods are not effective in coherent detection. So, in coherent detection these methods are costly, and with coherent detection it is easier to use PSK. It also reduces time delays. BPSK is the simplest form of PSK, as well as it supports 6 Mbit/s and 9 Mbit/s data rate [19].

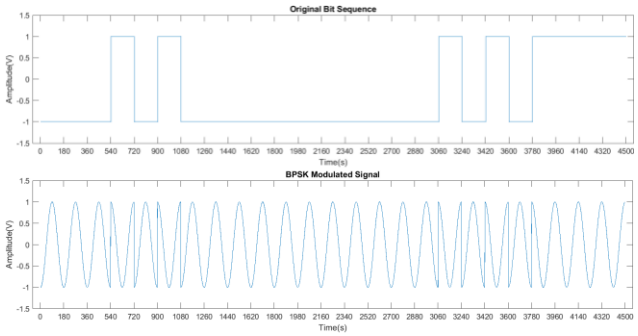


**Figure 2** Binary Phase Shift Keying

First of all, we need a low data rate to simulate the propose algorithm, so that we can verify our algorithm with low complexity with low data rate. In future work we will try to increase the data rate and try to get the benefit of bandwidth and power consumption by simulating PSK with higher data rate 12 Mbit / s and 18 Mbit / s by QPSK.

### 5.2 BLF FHSS System

When $T_S/T_H > 1$, i.e., the change of carrier frequency occurs repeatedly during the duration of the $T_S$ data symbol, then it is a system with the fast frequency hopping technique (FFH). Figure 3 shows a graphic operation diagram of the Bit Level Fast Frequency Hopping technique for an example of a code sequence pattern.

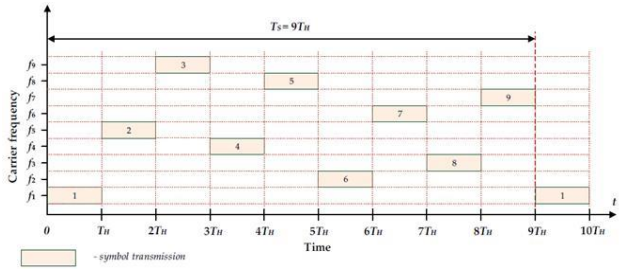


**Figure 3** Operation of BLF FHSS for an example code sequence pattern with a length of 9 ($T_S = 9T_H$)

In the FFH technique, the hop frequency:

$f_H = 1/T_H$ ……. (2)

In the case of non-coherent detection, to ensure the required orthogonality between the tones of the PSK modulation signal, a minimum distance between them being a multiple of $f_H$ should be used. This property ensures that no crosstalk occurs with the remaining hop frequency bands.

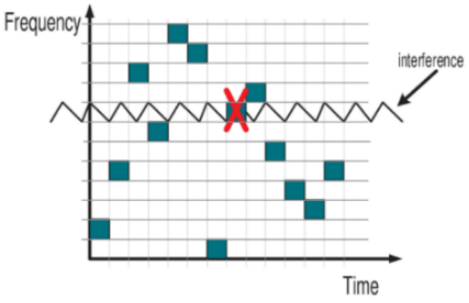


**Figure 4** BLF FHSS using BPSK system

An interfering signal would appear within the channel between the transmitter and thus the receiver [12] [11]. BLF FHSS could also be a selection spectrum technique, that uses a special frequency to transmit data quite 83 MHz Frequency agility depends on the facility to switch the frequency transmission of a sudden within the utilization of frequency (RF) bands. Divides the available 83.5 MHz spectrum (in most countries) into 79 discrete 1 MHz channels. The IEEE 802.11 standard specifies

data rates of 1 Mbps and a few of Mbps. So, as for a frequency hopping system to be 802.11 compliant, it must operate within the 2.4 GHz ISM band, and operate between 2.402 and 2.480 GHz [12].

RF channels are spaced 1 MHz and are arranged by channel number k according to the following formula: [19]

$f = 2402 + k$ *(MHz)* ……. *(3)*

Where, number of the channel of the Bluetooth system

$k = 0, \ldots\ldots\ldots\ldots, 78$

The hopping sequence is determined by the UAP (Upper Address Part) and LAP (Lower address Part) of a Bluetooth device address and the selected hopping sequence. The signal thus generated is then placed in the appropriate frequency sub-channel by means of a frequency conversion system for a time equal to the time of single hop time $T_H$ (or dwell time). The phase in the hopping sequence is determined by the Bluetooth clock. All physical channels are subdivided into time slots, whose length is different depending on the physical channel.

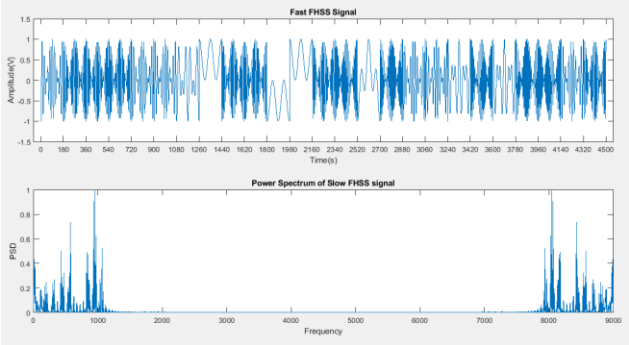


**Figure 5** Waveform and spectrum of BLF FHSS

In the receiver, the signal is reduced to the baseband in which BPSK demodulation occurs. The synchronization signal necessary to maintain the synchronization of the code sequence generator is obtained from the received signal by the code sequence synchronizer system. When $T_S/T_H > 1$, i.e., the change of carrier frequency occurs repeatedly during the duration of the $T_S$ data symbol, then it is a system with the BLF frequency hopping technique (FHSS).

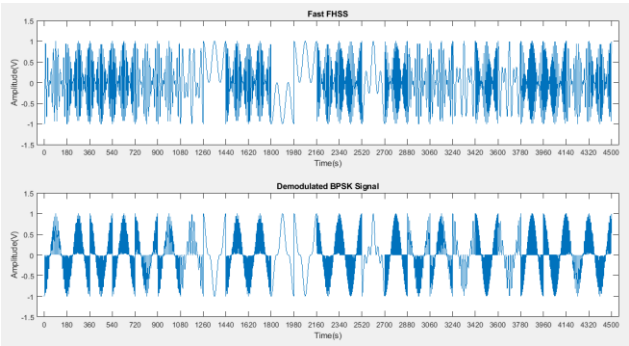


**Figure 6** BPSK retrieve from BLF-Frequency Hopping Spread Spectrum

## 6. CONCLUSIONS

Yun He et al. [16] has proposed the Double Window Spectrogram Difference method. A stop watch timer is utilized to measure the operation time of all methods, which run once for obtaining hopping frequency.

**Table 2:** The time that the method runs once.

| Methods | Time |
|---|---|
| DWSD | 1.055 |
| Generalized Rectangular time-freq. distribution | 18.14 |
| Re-arranged Spectrogram | 7.929 |
| STFT-WVD Joint algorithm | 2.303 |
| FHSS | 0.395 |
| BLF-FHSS | 0.375 |

It can be seen in Table 2, and figure 7, that the hopping frequency estimation performance of our proposed method has been improved, as well as its running time is shortest.

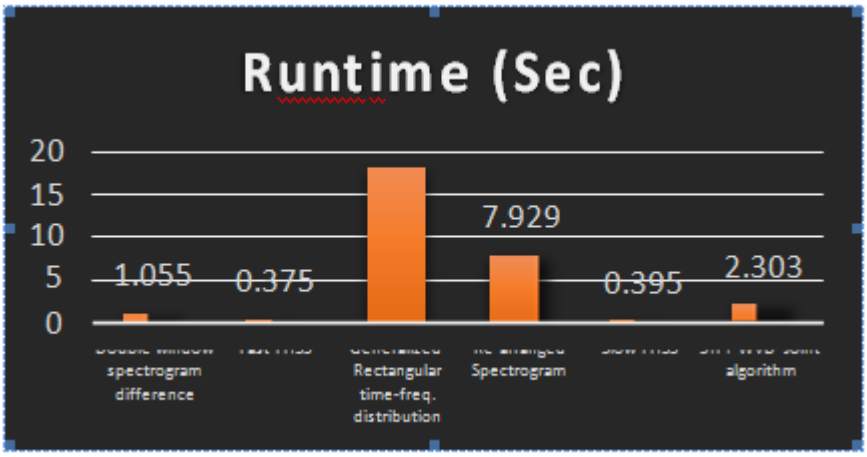


**Figure 7** Run times for the method runs once

Bluetooth devices can use the hopping kernel. In total, 6 types of hopping sequence are defined. In BLF frequency hopping, multiple hops are required to transmit one symbol, due to which its speed increases very much, and it quickly discovers the device that carries the inquiry.

## REFERENCES

[1] T A WWmon and S K Barton, "Receiver Techniques for Direct Sequence Spread Spectrum ISM Band Radio LANs", IEEE Proceeding, pp. 376-380, 1994.

[2] Sasikanth Avancha, Anupam Joshi, and Timothy Finin, "Enhanced Service Discovery in Bluetooth", IEEE Transaction on Communications, pp. 95-99, 2002.

[3] Igor Sedov, Stephan Preu B, Clemens Cap, Marc Haase, and Dirk Timmermann, "Time and Energy Efficient Service Discovery in Bluetooth", IEEE Proceeding, pp. 418-422, 2003.

[4] Hendnk R. Swanepoel, and Saurabh Sinha, "Design of a frequency hopped spread spectrum (FHSS) transceiver for cellular systems", IEEE AFRICON, pp. 567-571, 2004.

[5] Francisco Delgado, JosC A. RabadPn, Santiago PCrez, and Rafael Perez-JimCnez, "FHSS Transceiver over Wireless Indoor Optical Channels", IEEE Proceeding, pp. 1568-1573, 2004.

[6] Rozeha A. Rashid, and Rohaiza Yusoff, "Bluetooth Performance Analysis in Personal Area Network (PAN)", International RF and Microwave Conference Proceedings, Putrajaya, Malaysia, pp. 393-397, 2006.

[7] Jonathan R. Engelsma, and James C. Ferrans, "Bypassing Bluetooth Device Discovery Using a Multimodal User Interface", IEEE Proceeding, 2007.

[8] Andre Peters, and Andreas Heuer, "Time Efficient Service Discovery in Mobile P2P Architectures using Bluetooth", 19th International Conference on Database and Expert Systems Application, pp. 347-351, 2008.

[9] G. Bouzid, H. Trabelsi, Z. Elabed, and M. Masmoudi, "FPGA Implementation of FHSS-FSK Modulator", International Conference on Design &

Technology of Integrated Systems in Nanoscale Era, pp. 1-4, 2008.

[10] Syed Ali Hassan, and Mary Ann Ingram, "SNR Estimation for a Non-Coherent Binary Frequency Shift Keying Receiver", IEEE "GLOBECOM" 2009 proceedings, 2009.

[11] Yuh-Ren Tsai, "$M$-ary Spreading-Code-Phase-Shift-Keying Modulation for DSSS Multiple Access Systems", IEEE Transactions on Communications, Vol. 57, No. 11, pp. 3220-3224, November 2009.

[12] Handrizal Tanjung, and Ahmed N Abdalla, "Spread Spectrum Process using Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS)", National Conference on Postgraduate Research (NCON-PGR), pp. 18-27, 2009.

[13] Ahmed Jedda, Guy-Vincent Jourdan, and Nejib Zaguia, "Some Side Effects of FHSS on Bluetooth Networks Distributed Algorithms", IEEE Proceeding, 2010.

[14] Bin Zeng, and Lu Yao, "A Robust Estimation Algorithm for Device Discovery in Bluetooth Networks", 5th International Conference on Computer Science and Network Technology (ICCSNT), pp. 488-492, 2016.

[15] ZHAO Tonggang, LIU Kai, ZHOU Zheng, and PAN Dafa, "Research on the Frequency Hopping Algorithm Based on Long-distance Wireless Sensor Network", Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control, pp. 818-821, 2016.

[16] Yun He, Yang Su, Yuan Chen, Yao Yu, and Xiaolong Yang, "Double window spectrogram difference method: A blind estimation of frequency-hopping signal for battlefield communication environment", 24th Asia-Pacific Conference on Communications (APCC), pp. 439-443, 2018.

[17] Gaoyang Shan, and Byeong-hee Roh, "Performance Model for Advanced Neighbour Discovery Process in Bluetooth Low Energy 5.0-enabled IoT Networks", IEEE Transactions on Industrial Electronics, 2019

[18] Xiaopeng Tana, Shaojing Sub, and Xiaoyong Sun, "Research on Narrowband Interference Suppression Technology of UAV Network Based on Spread Spectrum Communication", IEEE International Conference on Artificial Intelligence and Information Systems (ICAIIS), pp. 335-338, 2020.

[19] J. MIKULKA, S. HANUS, Bluetooth and IEEE 802.11b/g Coexistence Simulation, Radio Engineering, Vol. 17, No. 3, September 2008.

**AUTHOR**

**Niti Singhal** did Master of Engineering in Electronics & Communication. Currently, she is PhD scholar in Vivekananda Institute of Technology, Jaipur, India.

**Dr. Kausar Ali** is working as a Professor in Vivekananda Institute of Technology, Jaipur, India.